

# USER ACCESS REQUEST AND RESPONSIBILITY STATEMENT

(FH Suppl 1 to AR 380-19)

## PRIVACY ACT

**AUTHORITY:** 10 U.S.C. 3013. **PURPOSE:** To control access, through password and user identification codes, to automatic equipment.

**ROUTINE USE:** To identify data processing and communications customers authorized access to data systems.

**DISCLOSURE:** Voluntary. Failure to provide information may result in denial of access to automation systems.

### PART I. ACTION REQUESTED (Filled in by ISSO).

a. Type of action: New Account ( ) Delete ( ) Change ( ) Renewal ( ) Contractor ( )

b. TSACS Login I.D. affected (if action is other than a new account): \_\_\_\_\_

c. Access requested on the following system(s) (check all that apply): Exchange ( ) TSACS ( ) DAISM ( ) PRWEB ( )

OROS ABC ( ) SIDPERS ( ) Telephone PIN: \_\_\_\_\_ SIPRNET: \_\_\_\_\_

d. For DAISM, enter Module name: \_\_\_\_\_

e. Other or special requirements: \_\_\_\_\_

### PART II. REQUESTOR INFORMATION (Filled in by user) except where noted, all entries are required for new accounts.

a. Name (Last, First, MI): \_\_\_\_\_

b. Title: \_\_\_\_\_ c. SSN: \_\_\_\_\_ d. Duty Telephone Number: \_\_\_\_\_

e. Office Symbol: \_\_\_\_\_ f. Building/Room Number: \_\_\_\_\_ g. Organization: \_\_\_\_\_

h. E-mail Address (required for TSACS accounts only): \_\_\_\_\_

### PART III. SECURITY ACCESS VERIFICATION (Filled in by Organizational Security Officer)

a. Security Access Level: NAC or ENTNAC ( ) SECRET ( ) TS ( )

b. Security Manager \_\_\_\_\_

PRINTED/TYPED NAME

DUTY PHONE

SIGNATURE

### PART IV. RESPONSIBILITIES REQUIREMENTS (Filled in by Requesting Organization and System Proponent).

As a potential user of Government information systems security resources, I am aware of the following responsibilities: I will use the resources only in the performance of my official duties. I will control and protect all data, software, hardware, passwords, copyrighted, or proprietary material to the best of my abilities. I will not use personally owned computers to access Government information systems security resources. I will immediately report suspected security incidents to my IASO. I will protect my user account name and password, and telephone access numbers at a level commensurate with the level of information being processed or accessed. I will abide by applicable security regulations and guidelines, and access only the resources authorized. I understand the password I receive as a result of this request is my personal access key and if I reveal my password to anyone, the password will be considered compromised and my access privilege suspended or revoked pending an investigation of the compromise.

a. Requesting Individual: I have read the above and will comply to the best of my ability.

Printed Name

Duty Phone

Date

Signature

b. Supervisor: I verify this access request is authorized.

Printed Name

Duty Phone

Date

Signature

c. IASO: I verify user has proper security clearance, understands security guidelines, is an authorized user.

Printed Name

Duty Phone

Date

Signature

d. Contracting Officer Representative (COR)/Contract Monitor (CM): I certify this request and authorization is required under the scope of the existing contract Company Name: \_\_\_\_\_ Contract Number: \_\_\_\_\_

Contract/access expires on (provide date required entry): \_\_\_\_\_

Printed Name

Duty Phone

Date

Signature

## Instruction for FH Form 380-23-R-E

### General. Type or legibly print all information.

Processing priority will be given to typed or neatly printed forms. Illegible forms will be returned without action, or will, at least, delay processing. Only legible FAX copies and requests with proper signatures will be processed. TSACS and Exchange E-mail passwords expire in six months. Exchange E-mail accounts not accessed within a 60 day period will be deleted. Exchange E-mail passwords for contractor personnel expire in six months and the account expires when the contract expires.

### Part I. Action Requested.

a. Indicate whether the request is to establish a new account or to delete or change an existing account. Provide any additional information in the special requirements section. To ensure our database is current, change requests should be submitted for name changes, transfers to other organizations, physical moves to another building, reorganizations (which may include everything in this section), and changes in telephone extensions. Requests for mass changes due to a physical move or reorganization can be accomplished by using one form with a separate listing of information from this section for all personnel affected. The organization's commander/ director/chief and Information Assurance Security Officer (IASO) must then sign the form in Parts III b and c.

b. Provide existing user's login ID when requesting the deletion or changing of an account or when establishing organization accounts and special accounts (i.e., "travel"). Login ID will be assigned when new accounts are established.

c. Access requested on following systems: Indicate the system(s) on which an account must be established, changed, or deleted. Provide any additional information in the special requirements section. When requesting PRWEB access, submit this form directly to contracting.

d. Name of the Installation Support Module (ISM.)

### Part II. Requestor Information.

a. User's full name.

b. User's title (i.e., Mr., Ms., or military rank).

c. User's social security number.

d. Building number and, if applicable, the room number for the user. A change request should be submitted if a user moves to another building due to reorganization/reassignment/promotion. Only the supervisor and the IASO need to sign the request in Parts III b and c for changes.

e. User's office symbol.

f. User's duty phone number. Provide the DSN and Commercial prefixes only for access to systems not physically located on Fort Huachuca. A change request should be submitted if a user's extension changes due to reorganization/reassignment/promotion. Only the supervisor and the IASO need to sign the request in Parts III b and c for changes.

g. User's organization. A change request should be submitted if a user moves to another branch or section within the same organization due to reorganization/reassignment/promotion. Only the gaining supervisor and IASO need to sign the request in Parts III b and c for changes.

h. List E-mail address for new TSACS accounts.

### Part III. Security Access Verification.

a. User's security access level. Minimal NACI investigation level required.

b. Security Manager or Facility Security Officer's name, duty phone, and signature.

### Part IV. Responsibilities Requirements.

a. Requesting Individual's full name and duty phone. The requestor must sign in this section.

b. Supervisor's full name and duty phone. The supervisor must sign in this section.

c. IASO full name and duty phone. The IASO must sign in this section. A copy of the IASO appointment memorandum must be on file in the DOIM.

d. For contractor personnel, provide the Contracting Officer Representative's (COR) or Contract Monitor (CM), full name and duty phone. For contractor personnel, the COR/CM must sign in this section. The COR is certifying a need for contractor personnel to access a specific Government system, such as E-mail or an ISM to fulfill contract requirements, company name, contract number and expiration date of the contract must be provided.